Universidad Zaragoza
1542

Trabajo Fin de Grado

INFRAESTRUCTURA DE ALTA DISPONIBILIDAD EN REDES DESPLEGABLES

Autor

Arturo Aguirre Moret

Directores

Director académico: Dr. D. Carlos Sánchez Tapia

Director militar: Cap. D. José Miguel Domínguez Rodríguez

Centro Universitario de la Defensa-Academia General Militar

Año 2017

Índice

Agradecimientos

En este punto, me gustaría agradecer la ayuda de todas aquellas personas que han hecho posible la elaboración de este Trabajo de Fin de Grado. Sin la ayuda y colaboración de los miembros de Regimiento de Transmisiones nº 21 y en especial de la 32 Cía., este trabajo no habría podido salir adelante. También me gustaría tener unas palabras de agradecimiento para el Cap. José Miguel Domínguez Rodríguez que ha sido de gran ayuda a través de su conocimiento y al Dr. D. Carlos Sánchez Tapia por su ayuda fundamental en la elaboración del TFG.

Resumen

El propósito del presente Trabajo de Fin de Grado es realizar un análisis de las redes desplegables de alta disponibilidad del Ejército de Tierra. Las redes desplegables en el Ejército de Tierra adolecen de falta de redundancia tanto en las conexiones como en los equipos que conforman la red, esto hace a las redes desplegables más sensibles y vulnerables. Por ello en este trabajo se buscan formas de solucionar los problemas que aparecen en los Nodos de SIMACET en su versión 5.

La metodología seguida en este TFG ha sido, primeramente, realizar un estudio sobre los componentes del nodo y, de forma simultánea, realizar entrevistas con los administradores con el fin de detectar y recopilar las vulnerabilidades, si es que poseen alguna, de los diferentes equipos. Posteriormente se han buscado soluciones a los problemas existentes, así como mejoras para conseguir que sean más operativos. Finalmente, se ha realizado un estudio de costes con el fin de cuantificar las mejoras.

La conclusión obtenida en el siguiente trabajo es que a pesar de buscar una reducción de medios y por tanto de costes en los nodos, las necesidades operativas y tácticas a las que se enfrenta el Ejército de Tierra hacen necesaria la incorporación de un segundo Nodo SIMACET v.5 de menor entidad para ser usado como respaldo, así como pequeñas modificaciones en los equipos.

Abstract

The purpose of this Final Degree Project is to analyse the high availability infrastructure on deployment networks of the Army. There is a lack of redundancy in both connections and devices in the deployment networks of the Army, which makes them more sensitive and vulnerable to failures. That is why in this project we aimed to solve the problems that appear on SIMACET Nodes on their 5th version.

In order to do this project, firstly we conducted a study on the components of the Node. Simultaneously, we interviewed the administrators to detect and compile the vulnerabilities, if existing, in the different pieces of equipment. Following, we looked for solutions to the existing problems, as well as improvements to make them more operational. Finally, we performed a cost analysis to quantify the improvements.

We concluded that, even if we look for a way to cut down on the resources, and therefore on the cost of the Nodes, due to the operational and tactical needs the Army faces, it is necessary to add a second SIMACET Node v.5, not so powerful, as a backup, as well as minor modifications to the equipment.

Índice de figuras

Índice de tablas

Tabla de acrónimos

Acrónimo	**Significado**
AAA	Artillería Antiaérea
ATQH	*At The Quick Halt*
AMPS	*Automated Mission Planned System*
BDT	Base de Datos Táctica
Bon	Batallón
BMS	*Battle Management System*
BGP	*Border Gateway Protocol*
BRI	Brigada
CCN	Centro Criptológico Nacional
CECOM	Centro de comunicaciones
CCMO	Centro de Control de Medios de Obtención
CIO	Centro de Información/Operaciones
CAOC	Centro de Operaciones Aéreas Combinadas
CPL	Centro de Personal/Logística
CNI	Centro Nacional de Inteligencia
COMFUT	Combatiente del Futuro
C2	*Command and Control*
CIS	*Communication and Information System*
Cía	Compañía
ET	Ejército de Tierra
EW	*Electronic War*
FMN	*Federated Mission Network*
GU	Gran Unidad
GACA	Grupo de Artillería de Campaña
Gr. Logístico	Grupo Logístico
ICC	*Initial CAOC Capability*
IPSec	*Internet Protocol Security*
IPS	*Intrusion Prevention System*
JC2IS	*Joint Command and Control Information Systems*
JFN	*Joint Force Command*
LCC	*Land Command Component*
LC	*Lucent Connector*
MALE	Mando de Apoyo Logístico al Ejército
MOPS	Mando de Operaciones
MNE	*Mission Network Element*
GRC-408E	Modelo de radio UHF
MIP	*Multinational Interoperatibility Programme*

NAS	*Network Attached Storage*
OG	Organismos Gubernamentales
ONG	Organismos No Gubernamentales
OTAN	Organización del Tratado del Atlántico Norte
Pel.	Pelotón
PU	Pequeña Unidad
RU	*Rack Unit*
RBA	Red Básica de Área
RRC	Red Radio de Combate
RTP	Red Táctica Principal
WAN PG	Red WAN de Propósito General
Secc.	Sección
SSL	*Secure Sockets Layer*
SAI	Sistema de Alimentación Ininterrumpida
SIM	Sistema de Información
TALOS	Sistema de mando y control de apoyo de fuegos
SECOMSAT	Sistema Español de Comunicaciones Militares por Satélite
GESTA	Sistema Táctico de Guerra Electrónica
SFP	*Small Form-factor Pluggable transceptor*
SAN	*Storage Area Network*
TN	Territorio Nacional
TFG	Trabajo Final de Grado
U. Helos.	Unidad de Helicópteros
U. Intel.	Unidad de Inteligencia
VPN	*Virtual Private Network*
WISE	*Web-Based Information Services Environment*

1. Introducción

En este Trabajo de Fin de Grado (TFG) se presenta un análisis de los problemas de red que afectan a las redes desplegables de alta disponibilidad del ET y se plantean soluciones para estos problemas, con la idea de que sea valorada su implantación en las unidades del ET.

El análisis se realiza haciendo hincapié en SIMACET, ya que es una de las partes claves de la red, al ser el cerebro de esta. Como se explicará más adelante, los nodos SIMACET proporcionan los servicios que utilizan los usuarios y es el motor por el que se ejecutan los procesos de aplicaciones tan importantes como la Base de datos Táctica de SIMACET (ANTARES), así como otras aplicaciones de diversa índole como pueden ser Exchange, JCHAT, SHAREPOINT, IGEOSIT o LOGFAS.

Dentro de las redes, los medios de transmisión son también elementos de gran importancia. La redundancia y el aumento de capacidad de transmisión tienen soluciones fácilmente aplicables en la actualidad como puede ser la modificación de la RBA para adaptarla a la tecnología IP, los enlaces Wimax o la adquisición de terminales satélites nuevos con nuevas capacidades.

Los terminales satélites son equipos de gran utilidad para las redes desplegables, ya que proporcionan una gran cobertura. Dependiendo del tipo de equipo que se utilice se consigue una cobertura mayor o menor: si se utilizan terminales militares se tiene cobertura en dos terceras partes del globo terráqueo, mientras que si los terminales satélite son civiles se puede conseguir cobertura mundial, aunque esto intenta evitarse por el poco ancho de banda que nos proporciona y su alto coste económico.

A pesar de que proporcionan buena cobertura y de que su uso está extendido en todas las unidades del ET, el uso de los terminales satélite para el enlace en la red desplegable plantea un gran problema: el ancho de banda que proporciona el satélite es muy limitado. Además, en la mayoría de las unidades los equipos de tierra de los terminales satélite de los que disponen, tampoco poseen suficiente ancho de banda como para responder a las crecientes necesidades que demandan los usuarios para poder compartir toda la información necesaria.

1.1. Motivación del Trabajo

La motivación principal de este trabajo es mejorar las comunicaciones militares y los sistemas de información que posee el Ejercito de Tierra y así brindar la oportunidad de que las telecomunicaciones militares españolas, y más concretamente las del ET, sigan en la vanguardia de las comunicaciones militares a nivel global.

Actualmente todas las unidades del ET disponen de Nodos de SIMACET para poder integrarse en los despliegues que realizan con el resto de unidades. El nodo más numeroso es el de Brigada, el cual, por las características que proporciona y el tipo de usuario al que va destinado, presenta muchas ventajas. Es por ello que el estudio se va a orientar a este tipo de nodos, para así conseguir que el trabajo tenga un mayor alcance.

1.2. Objetivos del proyecto

El objetivo principal del presente trabajo es recopilar y valorar las posibles mejoras técnicas y económicas en les redes desplegables de alta disponibilidad, principalmente en SIMACET, para su posterior implantación. Con ello se conseguiría modernizar la estructura de red buscando un coste asumible por el ET.

Con el fin de cumplir el objetivo principal, en el presente trabajo lo que se busca es rediseñar las redes desplegables para conseguir una redundancia eficaz que las convierta en estables y seguras ante los problemas que puedan surgir durante las operaciones o maniobras en las que sea necesaria su utilización.

Otro de los objetivos de este Trabajo de Fin de Grado es realizar un estudio conjunto de los Nodos de SIMACET de Brigada. Hasta la fecha, las modificaciones se han realizado por separado a cada uno de los equipos, lo que provoca que no se optimicen al máximo los recursos disponibles.

1.3. Metodología de la memoria

La metodología diseñada para resolver los problemas expuestos en el apartado anterior consiste en hacer un análisis minucioso equipo a equipo sobre todo de los Nodos de SIMACET, en concreto de los Nodos de Brigada. Se han elegido estos nodos porque, debido a su tamaño, son los más apropiados para un trabajo de estas dimensiones.

En el estudio lo que se busca es aprovechar la experiencia de los expertos en cada equipo para encontrar sus debilidades, proponer una solución y valorar la recomendación de su implementación.

Además, también se realizó un análisis de las capacidades teóricas de los equipos siendo necesario repasar los manuales del ET.

2. Generalidades

En los siguientes apartados se van a abordar los contenidos teóricos básicos para poder entender el desarrollo del presente Trabajo de Fin de Grado. En primer lugar se explicará qué son las redes desplegables de alta disponibilidad, que son el objetivo de análisis de este trabajo. Posteriormente se explicará qué es SIMACET y cómo eran las primeras versiones, pero centrándose sobre todo en la versión actual.

2.1. Red desplegable del ET

La red desplegable del ET es un conjunto de medios técnicos que permiten la comunicación a distancia entre los diferentes puestos de mando para facilitar, al jefe de la unidad desplegada, el mando y control de las unidades. Al ser desplegable, los equipos deben ser móviles y capaces de desplegarse en diferentes ambientes y terrenos manteniendo el enlace en cualquier parte del mundo.

Los medios que componen la red desplegable se pueden dividir en dos partes: los Sistemas de Información, que son los equipos que proporcionan los servicios a los usuarios, entre los que se encuentra SIMACET, y los Soportes, que son los equipos encargados de establecer el enlace y conformar la red, entre los que estarían los medios satélite y los medios radio.

2.2. SIMACET

La definición recogida en el manual del ET es la siguiente:

"*El Sistema de Información para el Mando y Control del Ejército de Tierra (SIMACET) permite a los Cuarteles Generales, Estados Mayores de las Divisiones y Brigadas (Grandes Unidades) y a las Planas Mayores de Mando de los escalones de Regimiento, Grupo Táctico, Batallón o Grupo (Pequeñas Unidades), planear, gestionar, controlar y dirigir las operaciones, así como obtener una visión coherente y homogénea del campo de batalla de todos los Puestos de Mando en tiempo operativo."* [1]

Se define nodo como el conjunto de medios hardware y software, capacidades, personal y procedimientos. La principal característica de los nodos es que disponen de una Base de Datos Táctica (BDT) que interactúa e intercambia información con la de otros nodos. El conjunto de varios nodos junto con los procedimientos de intercambio de información entre ellos constituye la red SIMACET. En la Figura 1 se pueden observar los diferentes tipos de Nodos existentes en el ET.

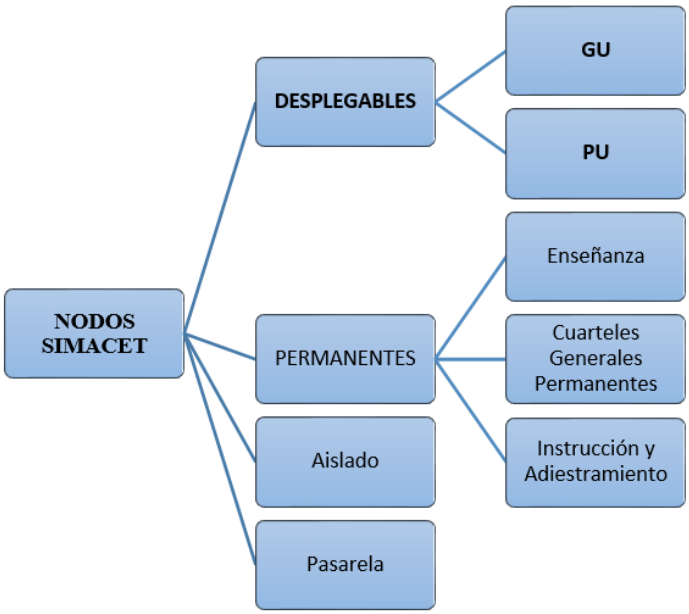

Figura 1. Tipos de Nodos SIMACET. Fuente: elaboración propia.

Aunque SIMACET se definió como sistema de información para grandes unidades (GU) y para pequeñas unidades (PU), en la práctica, hasta el momento solo las GU hacen uso de SIMACET. En lo que respecta a unidades de nivel inferior, el escalón Batallón e inferiores implementan el sistema de información BMS. Actualmente se está trabajando en la integración entre ambos para conseguir que el BMS alimente la base de datos de SIMACET. Como se observa en la Figura 2, el resto de sistemas de información están conectados a SIMACET permitiendo que sus datos sean compartidos en función de los privilegios otorgados.

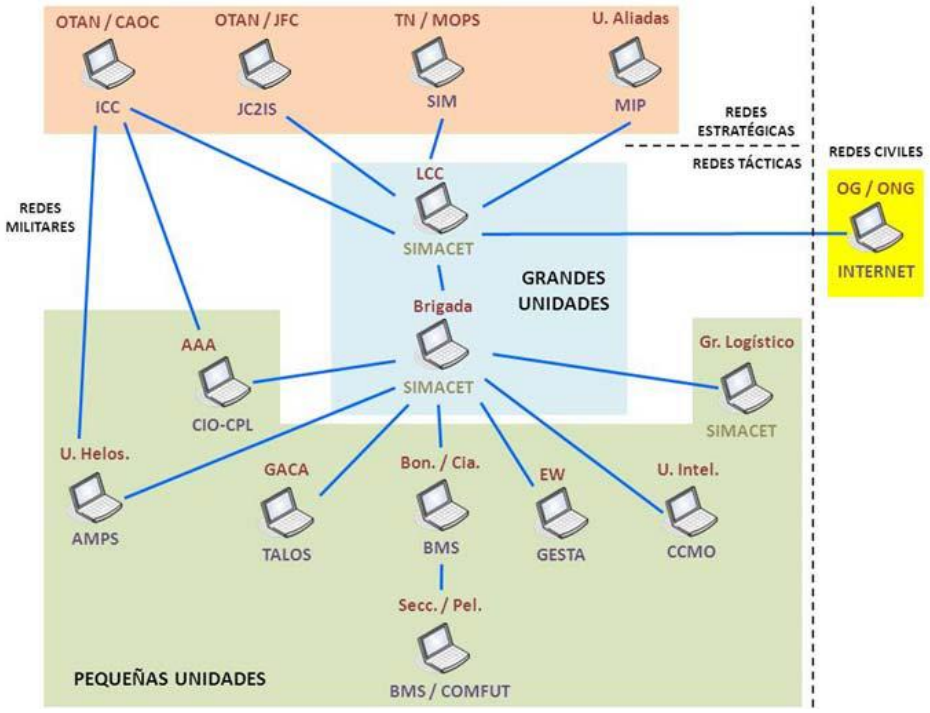

Figura 2. Esquema de los sistemas de intercambio de información en las redes militares [2]

Los principales objetivos que busca conseguir SIMACET son: una alta supervivencia del sistema, una visión común del campo de batalla, un sistema fiable de mensajería y una gran movilidad de los usuarios.

Para conseguir una alta supervivencia del sistema se toman diferentes medidas, como pueden ser la descentralización de los servidores, la compartición de información o la utilización de comunicaciones seguras. El uso de políticas de backup, que se explicará más adelante, permite que la información sea compartida entre todos los nodos que conforman la red, evitando así la existencia de un nodo central que sería más vulnerable a ataques, dificultando la recuperación de la información en caso de que cayera. Los datos, por tanto, se replican entre los nodos. El uso de redes de comunicaciones seguras (Red Básica de Área, Red Radio de Combate o SECOMSAT) permite que solo los usuarios de la red tengan acceso a esta, garantizando la confidencialidad, integridad y disponibilidad de la información.

La visión común del campo de batalla se consigue conectando las bases de datos entre sí, de manera que intercambian información entre ellas de forma automática gracias a la aplicación HIDRA y a que todas las bases de datos se encuentran al mismo nivel y no jerarquizadas.

A través de la aplicación XoMAIL se consigue tener una mensajería oficial que cumpla unos requisitos OTAN, tanto operacionales (control de sobretiempos, interoperabilidad con sistemas heredados, estandarización, extensión a entornos de bajo ancho de banda…) como de seguridad (información clasificada, posibilidad de cifrado…).

SIMACET consigue la movilidad de los usuarios ya que estos no pertenecen a un nodo, sino que pertenecen al sistema, por lo que tienen acceso a la información independientemente de donde se encuentren.

2.2.1. Primeras versiones

Desde comienzos de la creación y entrega del Programa SIMACET, allá por el año 2000, ha habido una serie de actualizaciones y readaptaciones con la finalidad de equilibrar el avance tecnológico y el coste económico, y dar respuesta de mayor capacidad a los usuarios. En los últimos años este avance se ha profundizado, desde las primeras versiones, donde todo se basaba en el hardware de los equipos, hasta la última versión, la 5.0, donde se virtualizan los servidores.

Existen 4 versiones de SIMACET[1]. La versión 3.2 fue la primera y la más sencilla de todas, ya que apareció cuando todavía se estaban desarrollando los sistemas de información militares en España (ver Figura 3). Apenas contaba con tres aplicaciones: Lotus Note para mensajería, NAS para crear y compartir carpetas y CANCERBERO como plataforma de acceso a las aplicaciones. En esta versión los servidores no tenían la opción de establecer controladores de dominio, por lo que se

[1] Número de versiones que han utilizado las unidades del ET.

conectaban físicamente dos controladores de dominio iguales a un clúster físico que trabajaba con dos cabinas de disco en espejo.

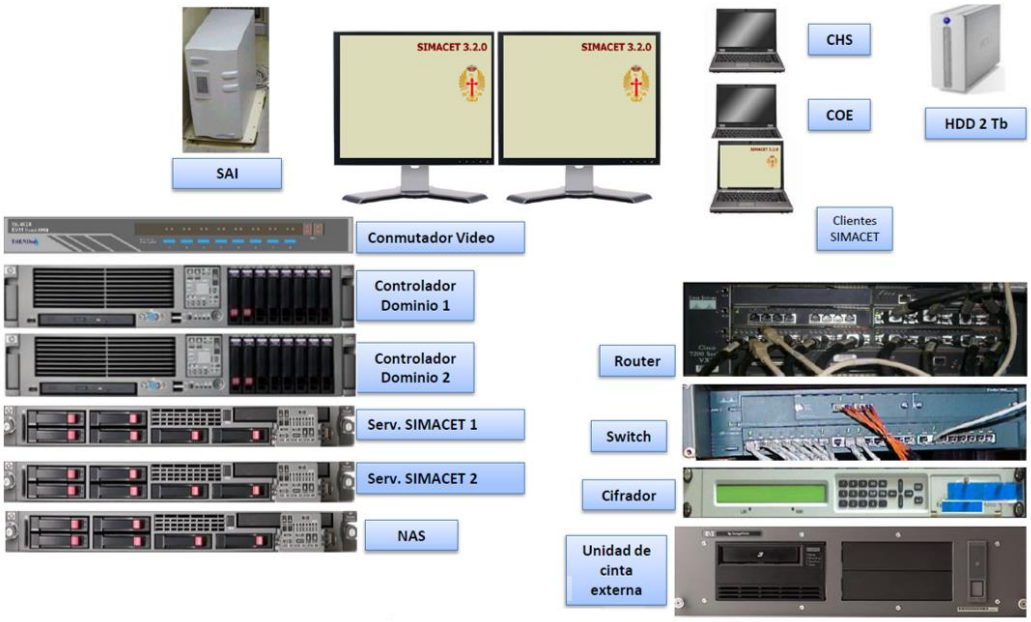

Figura 3 Componentes Nodo SIMACET V.3.2 de BRI [3]

Con la llegada de la versión 4.1 en 2013 se apreció un avance importante, ya que de las 3 aplicaciones que tenía en su primera versión SIMACET pasó a tener más de 30. Dentro de las aplicaciones, las novedades más destacables fueron JCHAT[2] y EXCHANGE[3] para la mensajería y la mejora de ALTAIR para la creación del fichero de misión. Al igual que en la versión anterior, se instalaron dos controladores de dominio y, además, se añadió un servidor de SHAREPOINT[4].

En el año 2015 aparecieron, prácticamente a la vez, las dos versiones de SIMACET que se encuentran actualmente en servicio en las unidades del ET, la versión 4.2 y la 5.0. Ambas versiones se ejecutan sobre Windows Server 2008 y tienen las mismas aplicaciones, pero la diferencia radica en el hecho de que la versión 4.2 no tiene los servidores virtualizados.

Además, las versiones de SIMACET 3.2, 4.1 y 4.2 van montadas sobre *shelter*[5], lo que presenta dificultades de acceso a los conectores. La versión 5.0 solucionó este problema siendo la primera en instalarse sobre un *rack*[6], con el

[2] JCHAT: mensajería instantánea entre usuarios.

[3] EXCHANGE: Es un servicio de mensajería al cual se le aplica Outlook. Es uno de los servicios más utilizados.

[4] SHAREPOINT: página web donde los usuarios pueden colgar y descargar documentos, con la idea de que sustituyan la utilización de las carpetas compartidas.

[5] Un *shelter* es un contenedor militar para el transporte de cargas. Normalmente se encuentran colocados en la parte de carga de los camiones militares.

[6] Un *rack* es un bastidor. A nivel militar un *rack* es un bastidor con configuración de sarcófago con la idea de proteger los equipos contra los golpes durante los traslados.

consiguiente ahorro de espacio, puesto que ahora ya no es necesario un camión solo para transportar el Nodo.

En las primeras versiones, había falta de redundancia de la información: si un servidor fallaba, se perdía el servicio alojado en el mismo. Por ello, y con el fin de hacer un uso más eficaz de los recursos disponibles, SIMACET avanzó hacia la virtualización de los servidores.

2.2.2. Versión 5

Como se ha comentado anteriormente, el Nodo SIMACET de Brigada es el más común en el ET, y la versión 5.0 es la que se pretende que adquieran todos estos nodos. Esta versión supone un salto tecnológico importante, pues se introdujo la virtualización [4] con las ventajas que ello supone, como son el ahorro de equipos físicos y un mayor aprovechamiento de los recursos.

El ahorro de los equipos físicos es significativo: el hardware necesario para un nodo de Brigada está compuesto por un servidor menos y no necesita dos controladores de dominio externos. Además, los dos switches son más potentes, el servidor de backup tiene más memoria y presenta la ventaja de que el SAI se conecta a una fuente de alimentación externa civil, no como en las versiones anteriores donde estaba conectada a un generador, bien del *shelter* bien militar. Esta configuración permite alojar el equipo dentro de un *rack* y no en un *shelter* como las versiones anteriores.

El mayor aprovechamiento de los recursos se consigue con la virtualización. Virtualizar aporta ventajas y posibilidades únicas en la actualidad. Permite reducir costes en prácticamente todos los campos de actuación de la administración de sistemas, desde la instalación y configuración de equipos hasta los procesos de copias de seguridad, monitorización, gestión y administración de la infraestructura. Además, disminuye el número de servidores físicos necesarios y el porcentaje de desuso de los recursos de los que disponen, aumentando su eficiencia energética. También brinda la posibilidad de centralizar y automatizar procesos cuya administración normalmente consume mucho tiempo, pudiendo aprovisionar y migrar máquinas virtuales de una manera rápida y fiable, manteniendo alta la calidad del servicio y bajo el tiempo de respuesta ante una caída del mismo.

Otra de las ventajas que presenta la virtualización es que se crean máquinas virtuales para sustituir el trabajo realizado por los equipos físicos, tanto los que se desea eliminar como los que adquieren nuevos cometidos. Una máquina virtual no viene a ser más que la representación de un PC físico, es decir, un sistema operativo al que llamaremos invitado junto con sus aplicaciones, datos, BIOS, etc. Las principales propiedades son:

- Encapsulación: la máquina se materializa en un conjunto de archivos.

- Independencia del hardware: el hardware físico subyacente se encuentra enmascarado.
- Aislamiento: las máquinas están totalmente aisladas unas de otras; si, por ejemplo, una se infecta con un virus, no se contagian los otros sistemas operativos.
- Escalabilidad: presentan gran facilidad de expansión de capacidad.

A lo largo del trabajo iremos viendo como todas estas propiedades son de utilidad en los diferentes equipos, desde el aislamiento para los firewalls a la encapsulación para distribuir la memoria y conseguir copias. El funcionamiento de los nodos en su última versión, la versión 5.0, está por lo descrito anteriormente, altamente ligado a la virtualización.

2.2.3. Composición de un Nodo SIMACET V.5 de Brigada

Los Nodos de Brigada están diseñados para dar servicio a un máximo de 254 usuarios, aunque realmente solo tienen necesidad de dar servicio a entre 70 y 80. Los nodos se configuran para buscar redundancia en los servicios por lo que cuentan con más equipos de los necesarios, buscando que en caso de que alguno de los equipos del nodo falle haya otro que pueda realizar su función.

A pesar de las diferentes versiones existentes en el software, el hardware se ha mantenido constante, renovando los equipos solo por una versión posterior del mismo equipo. Aunque los nodos se encuentran dentro de *racks* modulables, los componentes siempre se colocan en la misma posición para facilitar a los administradores el trabajo. En la Figura 4 podemos ver una representación, tanto en la parte frontal como posterior del *rack*, de los equipos que componen un nodo. La composición, empezando de arriba abajo es la siguiente:

- Dos switches de acceso ALLIED TELESIS AT-x610 24x:
  - Veinticuatro interfaces Gb Ethernet.
  - Dos interfaces de fibra óptica a Gb Ethernet.
- Dos servidores HP PROLIANT DL 380P GEN8:
  - Dos HDD de 146 GB RAID 1 almacenamiento interno.
  - Procesador INTEL XEON ES- 2650 8 CORE 2Ghz.
  - Adaptador HBA 8Gb conector SFP.
- Servidor STOREONCE BACKUP HP 2700:
  - Cuatro HDD 2TB.
- SAI HP 5500RX.

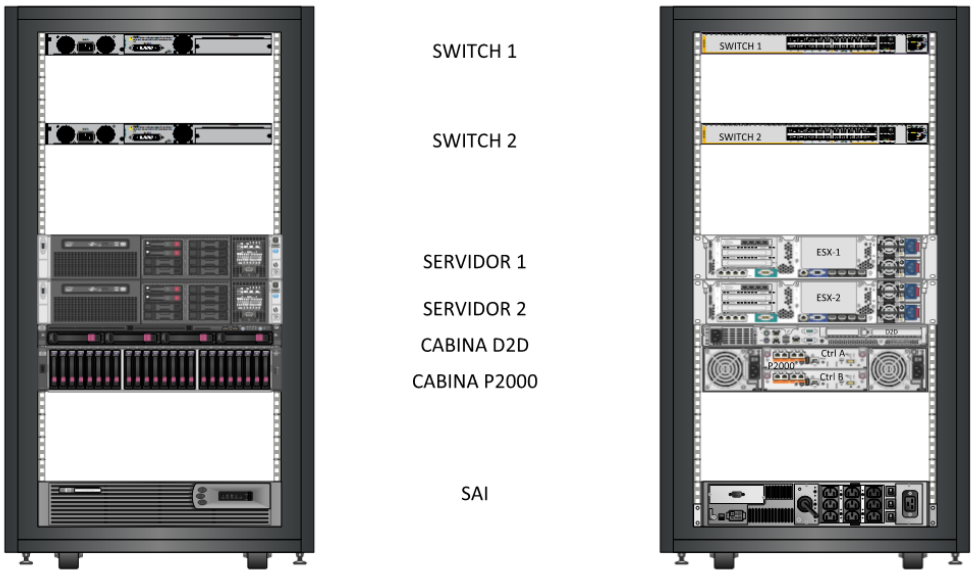

Figura 4. Módulo servidor SIMACET V.5 BRI [5]

Los equipos se encuentran interconectados mediante diferentes medios para proporcionar redundancia en el enlace. El diagrama de enlace que se representa en la Figura 5 representa las diferentes conexiones que se pueden establecer para conectar los módulos de SIMACET en un Centro de Transmisiones. Aunque esta figura sea una propuesta, la mayoría de las conexiones ya se están implementando de esta forma. Como podemos observar, se utilizan todas las redes de las que dispone el ET, desde la Red Táctica, la Red Estratégica o la Red Radio de Combate hasta enlaces intrateatro o en espejo.

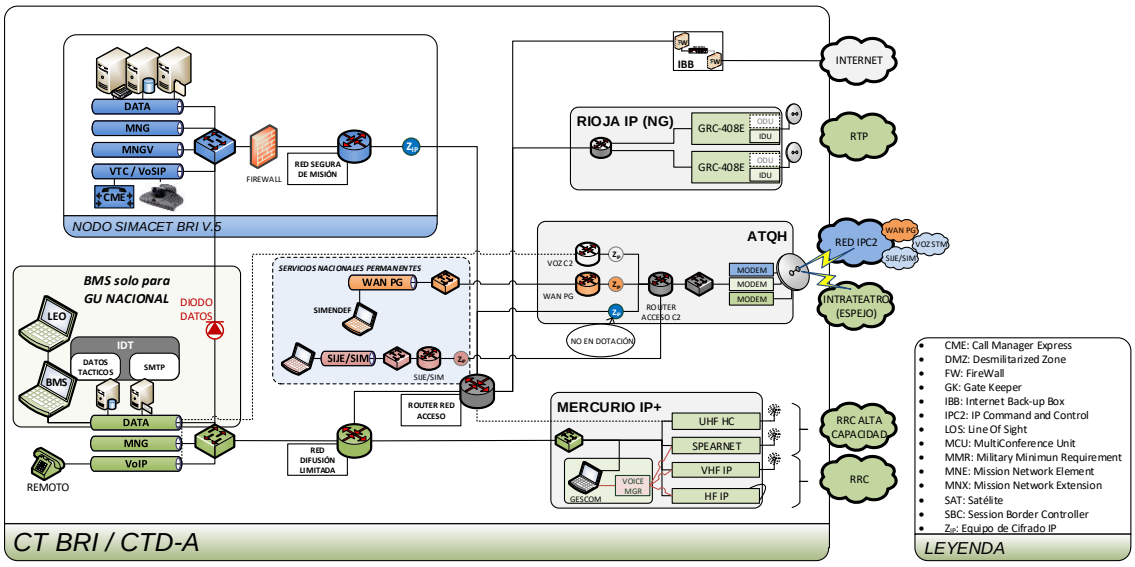

Figura 5. Propuesta de futuro para un CT de Brigada [2]

2.2.4. Tendencia futura

Actualmente el grado de virtualización de los nodos es amplio, pero en el futuro se está buscando aumentarlo. Por ello, la tendencia futura es virtualizar todos los componentes de un nodo SIMACET, en la llamada versión 6. Sin embargo, hay que recordar que virtualizar también trae consigo otros inconvenientes como la complejidad técnica a la hora de trabajar con los equipos y la necesidad cada vez mayor de tener a personal más especializado para su administración.

3. Estudio de hardware de un Nodo SIMACET V.5 de BRIGADA

En el presente Trabajo de Final de Grado se ha hecho un análisis de las redes desplegables del ET, siendo la parte del hardware un punto muy importante dentro de estas. Hasta hace unos años hardware y capacidades estaban altamente ligados, pero con la virtualización esta relación deja de ser tan estrecha. Aun así, el hardware representa un componente imprescindible de los Nodos de SIMACET.

En los siguientes apartados se va a proceder a realizar un análisis de los diferentes equipos físicos que conforman un Nodo SIMACET V.5 de Brigada, haciendo uso de entrevistas a los suboficiales administradores[7] de los equipos para conseguir información procedente de personal altamente cualificado y con experiencia en el manejo de los equipos en las condiciones a las que los pone a prueba el ET. También se va a realizar una búsqueda de documentación en diversas fuentes con objeto de identificar los posibles problemas que pudieran aparecer en los equipos y por tanto suponer fallos críticos de los mismos.

3.1. Análisis del SERVIDOR HP PROLIANT DL380P GEN8

El Nodo SIMACET V.5 de Brigada está compuesto por dos servidores HP PROLIANT DL380P GEN8 [6] (ver Figura 6). Estos servidores son los que tienen cargados los servidores virtualizados de SIMACET y los controladores de dominio.

Figura 6. Servidores Nodo SIMACET V.5 BRI. Fuente: elaboración propia.

Cada servidor posee 16 procesadores Intel Xeon CPU E5-2650[8]. La capacidad de cada servidor es de 192GB de memoria RAM. Esta capacidad es más que suficiente para dar los servicios requeridos a nivel Brigada. La ecuación utilizada para decidir el número de servidores necesarios responde a

[7] Ver Anexo 6. Entrevistas.
[8] Ver Anexo 3 con las características técnicas.

$$n=n+1$$

siendo *n* el número de servidores necesarios para el correcto funcionamiento del nodo.

Debido a la entidad a la que da servicio este nodo, tiene entre 70 y 80 usuarios, aunque en algún ejercicio en particular puedan ser un número mayor, no superando en ningún caso los 204 usuarios[9].

Tras las entrevistas con los suboficiales administradores de los servidores[10], se ha llegado a la conclusión de que estos equipos no presentan problemas en cuanto al trabajo que se les requiere, es decir, tienen la suficiente potencia. Por el contrario, presentan el inconveniente de su sensibilidad a trabajar en condiciones poco favorables, como en sitios muy cálidos o estar desplegándose múltiples veces en cortos períodos de tiempo. Debido a sus altas prestaciones, los equipos se calientan en exceso, requiriendo asistencia externa para una adecuada refrigeración. Además, es necesario que el equipo de refrigeración sea potente, puesto que cuando van montados sobre *shelter* los equipos que llevan instalados resultan insuficientes. El segundo problema es debido a los conectores de la fuente de alimentación que no están pensados para estar montándose y desmontándose, lo que en muchas ocasiones da lugar a fallos. Estos problemas se abordarán en el apartado 6.1.

3.2. Estudio del array de discos ARRAY DE DISCOS HP STORAGEWORKS P2000 G3

Los nodos de SIMACET v.5 de Brigada poseen un array de discos, en el nodo sobre el que se realiza el estudio. Este equipo es el HP STORAGEWORK P2000 G3 compuesto por 24 discos de 900GB como se puede ver en la Figura 7, por lo que tiene un espacio de almacenaje de 21,6TB, capacidad más que suficiente para el uso requerido.

Figura 7. Array de discos Nodo SIMACET V.5 BRI. Fuente: elaboración propia.

[9] 256 es el número de direcciones IP con las que puede trabajar ya que la máscara de subred es /24; y a este número hay que restarle dos direcciones, una para el propio equipo y otra para broadcast, además también se reservan otras 50 direcciones para la gestión de la red.

[10] Ver Anexo 6.1.

En un nodo todos los equipos se encuentran duplicados y desplegados en forma de clúster[11] para evitar que el fallo de uno de los equipos deje inoperativo al nodo, a excepción del array de discos y del servidor de backup. En el caso del primero, esto se debe a que, atendiendo al funcionamiento del equipo, no se considera necesario un segundo equipo, ya que por su propia configuración funciona como si fueran equipos separados; mientras que en el caso del segundo se debe a cuestiones económicas. Normalmente los discos utilizan la configuración de RAID 5, pero al utilizar un número elevado de discos es mejor trabajar con paridad dual, por el aumento de la probabilidad de que se produzca un fallo simultáneo en dos discos, y por eso, en el Nodo SIMACET V.5 se utiliza la configuración de RAID 6. Este tipo de configuración divide la información en bloques y los distribuye junto con dos bloques de paridad entre los diferentes discos que forman la matriz. Además, este modelo de array de discos permite que al extraer un disco dañado e introducir uno nuevo, automáticamente se copia la información que se encontraba en el disco extraído.

A pesar de esto, sigue existiendo la debilidad de que toda la información se guarda en un solo equipo, con el consiguiente riesgo de que pueda ser destruido o una incidencia en el firmware provoque la perdida de toda la información almacenada. Es posible que un fallo eléctrico provoque que los equipos se apaguen de manera repentina produciendo una pérdida de los metadatos que almacenaban la información que indica donde están situados los datos. Durante las maniobras TIWAR 2017[12] apareció este problema y, a pesar de los múltiples intentos, no se encontró otra solución más que borrar todos los datos y volver a programar todo de cero. Esto supone tener imágenes actualizadas del estado de los discos para minimizar la pérdida de información. Por tanto, la única solución a este problema es la prevención, y por ello es importante contar con copias de seguridad de los datos con los que se está trabajando.

Otro de los problemas que pueden afectar al array de discos por falta de corriente eléctrica es que se pierda la información de las controladoras de discos. Puesto que existen dos controladoras, al encontrarse duplicadas es difícil que caigan ambas por este motivo, aunque no es descartable. Este problema no tiene solución más que utilizar la segunda copia del equipo, la copia de seguridad, pero ya se empezaría a trabajar sin otro respaldo en caso de que volviera a fallar. Este puede ser un problema en los nodos de Brigada y de División, ya que solo cuentan con un array de discos, por ello en el apartado 6.2 se abordará la incorporación de un segundo array en estos nodos.

Tras realizar una entrevista con los suboficiales administradores (ver Anexo 6.2. Entrevista Sargento 1º Zuluaga administrador HP STORAGEWORKS P200 G3) de los diferentes nodos, a la pregunta de cuál es el componente que más problemas

[11] Clúster de alta disponibilidad: es un conjunto de dos o más máquinas que mantienen una serie de servicios compartidos y están constantemente monitorizándose entre sí.

[12] Ejercicio de escuelas prácticas CIS del RT-21.

presenta hubo unanimidad en la respuesta: los discos de almacenamiento son elementos delicados, y en el caso de que el equipo se encuentre desplegado en el campo o trasladándose se pueden llenar de polvo o se rayase y quedar inoperativos. Hasta la fecha la sustitución del disco dañado por uno nuevo es la única solución posible, y por ello se recomienda disponer de recambios durante los ejercicios. Estos costes se detallan en el apartado 7 de esta memoria.

3.3. Estudio del servidor de backup

Los nodos SIMACET V.5 cuentan con un servidor de backup para realizar las copias de seguridad. El modelo que se encuentra en los nodos de brigada es el HP STOREONCE 2700 [7], formado por cuatro discos de 2 TB con un total de 8 TB de memoria de backup (ver Figura 8). En los nodos de División y de Cuerpo de Ejército el modelo utilizado es diferente: es el HP STOREONCE 4700 con 24 TB, divididos en 12 discos.

Figura 8. Servidor de Backup Nodo SIMACET V.5 BRI. Fuente: elaboración propia.

Al igual que el array de discos, el servidor de backup no se encuentra redundado, por lo que, en caso de quedar inoperativo, el nodo no dispondría del servicio de backup, aunque podría seguir funcionando sin él.

El problema más común observado en estos equipos es la actualización de las licencias, ya que es necesaria la licencia de Backupexec[13], sin la cual el equipo no puede funcionar. La adquisición de las licencias para los equipos la realiza el Parque Central de ET y posteriormente las reparte a las unidades.

3.4. Estudio de los Switch

En los nodos podemos encontrar dos switches AT-X610-24TS [8] (ver Figura 9). En el Anexo 2 vienen explicadas en detalle las características completas de este modelo de switches, aunque los aspectos más importantes se recogen en este

[13] Es la aplicación para la ejecución de copias de seguridad y restauración para servidores Windows; el programa encargado de organizar la información almacenada en el servidor de Backup, actúa como una *libraría de brazo robótico*. La versión es *SYMANTEC BACKUP EXEC 2012* (AGENT FOR WINDOWS SYSTEM, LIBRARY, MSFT EXCHANGE, SERVER).

apartado. Estos equipos disponen cada uno de 24 puertos de Gigabit Ethernet, por lo que entre ambos el nodo dispone de 48 salidas RJ-45, un número insuficiente. Para poder hacer frente al número de puertos de switch necesarios para conectar los diferentes equipos de la red, los Nodos de SIMACET en su versión 5 utilizan la virtualización. Creando uno o varios switches virtualizados en los servidores consiguen gestionar el direccionamiento de los equipos de la red para que cada equipo llegue por un puerto y no haya problemas. Esto también se utiliza para crear diferentes VLAN como podemos ver en la figura 9.

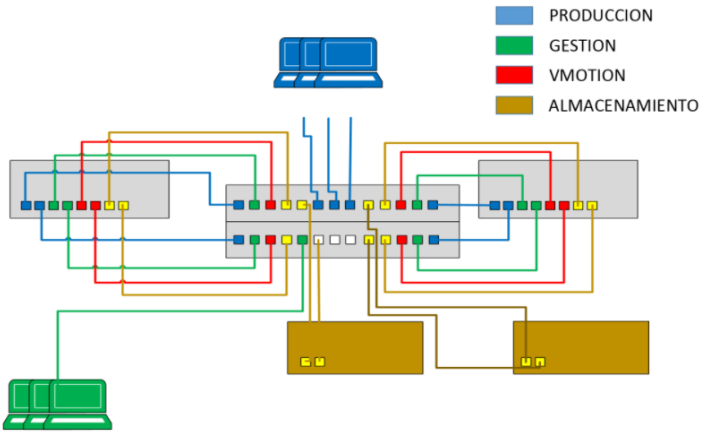

Figura 9 VLAN en los switch del Nodo SIMACET V.5 [9]

Además de los puertos RJ-45, cada switch también cuenta con dos puertos de fibra óptica multimodo. Los conectores de fibra se utilizan entre los switches cuando se busca en las conexiones una mayor velocidad o la distancia entre dos equipos es mayor de 100 metros[14].

Figura 10. Switches Nodo SIMACET V.5 BRI [8]. *Fuente: elaboración propia.*

Después de analizar los equipos AT-X610-24TS se ha llegado a la conclusión de que no presentan ningún fallo en su funcionamiento y además lo hacen de manera muy correcta. También se ha llegado a la conclusión de que sus capacidades no limitan las del Nodo SIMACET V.5 de Brigada, ya que las bocas UTP podrían ser

[14] 100 metros es la distancia máxima a la que se pueden conectar dos equipos con cable UTP debido a las pérdidas de información que se producen en este con la distancia.

un problema, pero la virtualización las resuelve de manera satisfactoria. Por tanto, se recomienda no realizar ninguna modificación de estos equipos hasta que no resulten obsoletos.

3.5. Estudio del Sistema de alimentación (SAI R/T3000VA G2)

Los sistemas de alimentación ininterrumpida (SAI) son dispositivos encargados de proporcionar energía de calidad y de forma continuada a los equipos que la requieran para conseguir un buen funcionamiento del equipo o para evitar su avería. Los SAI son por tanto un elemento importante para los equipos electrónicos que conforman las redes del ET, ya que los protegen de subidas o bajadas de tensión y de interrupciones repentinas de alimentación eléctrica. Un SAI es por tanto una batería grande que se va recargando mientras alimenta a los equipos.

Los SAI son equipos delicados y por tanto pueden presentar fallos debidos a su utilización. Estos fallos son bastante comunes y se enumeran en los siguientes párrafos. Además, la naturaleza de los fallos se repite bastante, pudiendo observar durante las prácticas algunos de ellos. De hecho, un 90% de los problemas observados durante la elaboración de este trabajo tenían algún tipo de relación con los sistemas de alimentación.

El principal problema que presentan los SAI es que, al estar conformados por baterías, tienen una capacidad limitada en el tiempo para proporcionar alimentación a los equipos y con el paso de los años esta se ve reducida por hacer uso de las mismas llegando incluso a averiarse o romperse, en cuyo caso el equipo quedaría inutilizado hasta que se reparara o sustituyera por otro nuevo.

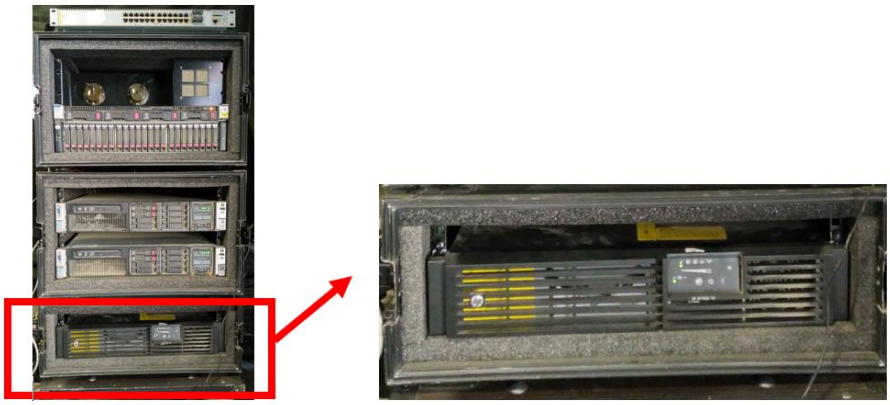

Figura 11. SAI R/T3000VA. Fuente: elaboración propia.

El problema de que el SAI tenga una duración corta o poca capacidad de alimentación de los equipos, es común dentro de los Nodos de SIMACET V.5 en el ET, ya que los equipos utilizados fueron adquiridos hace bastantes años y su vida útil se ha visto reducida. En el caso del SAI R/T3000VA[15] (ver Figura 11), que es con la

[15] Ver Anexo 4 Características SAI R/T3000VA.

que cuenta el Nodo SIMACET de Brigada la capacidad está probada como insuficiente. Para el arranque de un nodo se necesitan 60 minutos, de los cuales 30 minutos se destinan al encendido de las máquinas físicas y 30 minutos a las virtuales. Por el contrario, el proceso de apagado de un Nodo es mucho más largo, ya que se puede llegar a necesitar el doble de tiempo para apagarlo que para encenderlo, por lo que estamos hablando de un tiempo de 2 horas. Por tanto, aun con un SAI R/T3000VA nuevo, la capacidad que nos ofrece es insuficiente. El problema de la capacidad del SAI se abordará en el apartado 6.5.

Un segundo problema al que deben enfrentarse los SAI son los picos de tensión. En caso de que se produzca uno, estos pueden averiarse, dejando al nodo sin una fuente de alimentación alternativa. Una subida de tensión puede dejar inutilizado el SAI y, por consiguiente, los equipos a los que proporcionaba el servicio quedarán fuera de servicio hasta que se cambien los SAI para evitar posibles daños mayores.

Otro de los problemas a los que deben hacer frente es la detección de alarmas. El modelo R/T3000VA dispone de un led que indica el estado de la batería, ya sea cargada, descargada o a media carga. Además, dispone de una alarma sonora. Los equipos presentan problemas a la hora de avisar a los administradores cuando entran en funcionamiento porque o bien el led no es apreciable dentro de un *rack* o bien el ruido de la alarma sonora es insuficiente, sobre todo si tenemos en cuenta el ruido que se puede generar por el funcionamiento de los servidores. Una posible solución a estos problemas se abordará en el apartado 6.5.

4. Estudio de software de un Nodo SIMACET V.5 de Brigada

Como se ha mencionado anteriormente, el software está adquiriendo cada vez mayor importancia en los nodos y, por tanto, cuando se realiza un análisis de los Nodos SIMACET V.5 de Brigada no puede faltar un análisis del software. Puesto que hay múltiples equipos dentro de este tipo de nodos, solo se va abordar en este apartado el software relacionado con SIMACET propiamente dicho, y no con el propio del funcionamiento de cada equipo, puesto que eso ya se ha hecho en los estudios realizados en el apartado 3.

El software analizado tiene gran relación con la virtualización y los problemas que aparecen responden en gran medida a los problemas que puede presentar la virtualización a la hora de crear máquinas. Aunque la virtualización es algo que lleva muchos años funcionando, en el ET es algo relativamente nuevo. Además, hay que tener en cuenta las diferencias en la utilización de estas respecto al uso que pueden hacer empresas civiles. Por ejemplo, en el caso de una empresa civil, cuando se crea una máquina virtual esta permanece inalterada durante un largo periodo de tiempo y, por tanto, los fallos se acaban solucionando. Sin embargo, en el ET las máquinas son creadas para cada maniobra y después se eliminan siendo su configuración diferente para cada ejercicio, con lo que aparecen diversos problemas de programación que son difíciles de gestionar pues cada vez se trabaja con unas variables diferentes.

Como se ha mencionado en el párrafo anterior, los problemas pueden tener una naturaleza muy diversa. Aun así, hay algunos que se repiten, como los relacionados con la tarjeta de red del controlador de dominio. Cuando se reinicia el equipo, algo que puede pasar por un fallo de suministro eléctrico, la tarjeta de red del controlador de dominio se deshabilita, por lo que el equipo hace que el nodo deje de funcionar. Esto se debe a que el controlador de dominio es el cerebro del nodo, y por eso se encuentra redundado con un segundo controlador. De hecho, es probable que ocurra que cuando cae uno el otro también lo haga por los mismos motivos.

Otra de las dificultades a las que tienen que hacer frente los sistemas de telecomunicaciones militares, son los usuarios. El interfaz de usuario en todas las versiones de SIMACET no es lo suficiente intuitivo y sencillo para que los usuarios puedan desenvolverse con el sistema y sacar el máximo partido de los recursos que ponen a su disposición los equipos. Esto repercute en el correcto funcionamiento de los nodos, ya que, en muchas ocasiones, los problemas relativos al software deben ser detectados por los usuarios y no por los administradores. Un claro ejemplo de ello son los problemas relacionados con la mensajería del servidor EXCHANGE. Este tipo de servidor no acaba de funcionar correctamente en los Nodos de SIMACET y deben ser los propios usuarios los que detecten los fallos en la aplicación y se lo

notifiquen al administrador para que los solucione. Estos fallos se abordarán en el apartado 6.6.

Además de los problemas debidos a la virtualización, los nodos tienen los problemas comunes a los equipos electrónicos, y es que necesitan licencias actualizadas para poder funcionar. En el ámbito militar, el software debe estar certificado (no se puede utilizar software libre[16]) por lo que en muchas ocasiones el abanico de ofertas disponibles se reduce a unas pocas o incluso una sola versión de licencia. Por tanto, con este requisito se elimina la posibilidad de utilizar software libre gratuito y el ET se ve en la obligación de pagar costosas licencias[17]. También se debe tener en cuenta que la versión adquirida sea compatible con el resto de versiones existentes en el nodo, ya que en caso contrario se producen fallos en el funcionamiento del mismo. Estos problemas, junto con los primeros relacionados con la virtualización, se van a tratar en el apartado 6.6.

[16] La OTAN no acredita software libre, por lo cual, a nivel nacional el CCN (elemento dependiente del CNI) ha creado diferentes STIC para acreditar el software de los Nodos SIMACET V.5. Las STIC son material clasificado y por tanto no pueden ser incluidas en el presente trabajo.

[17] Las licencias de software empleadas por los nodos SIMACET V.5 así como su precio están recogido en un documento clasificado como *Mission Secret* o Reservado y por tanto no puede ser incluido en el presente trabajo.

5. Estudio de los componentes en la red

Cuando analizamos los Nodos SIMACET V.5 de Brigada, no podemos olvidarnos de analizar también los diferentes equipos de la red que los unen y que pueden presentarse como cuellos de botella para sacar el máximo partido a los equipos o suponer falta de redundancia. Como vemos en la Figura 12, están compuestos por más equipos que los del *rack* de servidores. Estos son los elementos de la red que se encuentran entre los servidores y los equipos de transmisión. Por tanto, cuando hablamos de Nodos SIMACET V.5 debemos tener en cuenta que, de dotación en las unidades, estos nodos también disponen de un firewall (CISCO ASA 5525X), un cifrador y dos routers, uno negro[18] y otro rojo[19].

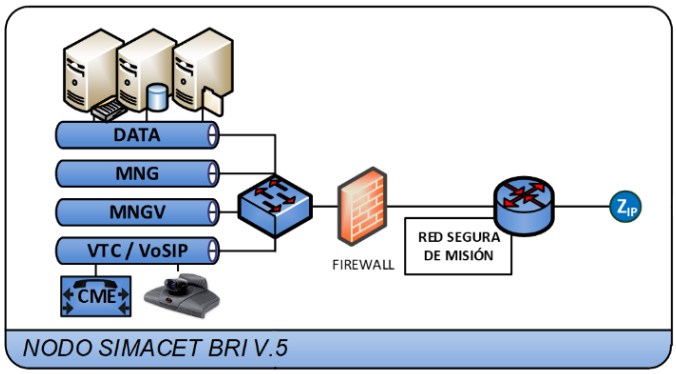

Figura 12. Componentes de Red de un Nodo SIMACET V.5

5.1. Estudio de los Firewall

Un firewall o cortafuegos es un dispositivo de seguridad de la red que monitoriza y controla el tráfico entrante y saliente y decide si este puede ser dañino para la red y debe ser bloqueado o, en caso contrario, debe permitirlo, es decir, fuerza una política de seguridad entre varios dominios. Por ello debe ser el único punto físico en común entre los distintos dominios de seguridad, y por tanto no deben existir puertas traseras.

En los últimos años las amenazas cibernéticas han evolucionado desde vectores de ataque simples hasta sujetos capaces de construir malware persistente, muy sofisticado, con capacidades de infección en múltiples áreas. Para poder ofrecer una prevención eficiente, las soluciones actuales de seguridad necesitan comprender y gestionar todas las fases en la cadena de ataque.

Actualmente, está apareciendo una nueva generación de aplicaciones capaces de evadir la detección que ofrecen los firewalls o cortafuegos tradicionales que permitían establecer políticas de seguridad basadas fundamentalmente en puertos y

[18] Un router negro es aquel que se encuentra después del cifrador y, por tanto, todos los datos que pasan por el van cifrados.

[19] Un router rojo se encuentra antes del cifrador, por lo que a diferencia del router negro los datos que pasan por este router son visibles a todo aquel que se conecte a él.

protocolos. Hasta hace poco tiempo, esta aproximación era válida pues lo normal era que por el puerto 80 pasara sólo la navegación web y por el puerto 443, el tráfico SSL. Sin embargo, muchas de las nuevas aplicaciones de la Web 2.0[20] utilizan técnicas evasivas como *port hopping*, tunelización/emulación de otras aplicaciones, etc., para burlarse de las reglas de los cortafuegos tradicionales. Como resultado de todo ello, no se pueden identificar o controlar las aplicaciones que están corriendo realmente en la red, y esta falta de visibilidad y control puede generar fugas de datos y un aumento de las amenazas.

En el siguiente capítulo se va a realizar un análisis de las vulnerabilidades de los firewall CISCO ASA 5525X [10], para posteriormente valorar si cumplen con los requisitos que espera y necesita el ET.

El firewall CISCO ASA utiliza el software *Adaptive Security Appliance* diseñado para proporcionar funciones de firewall de clase empresarial, tales como funciones IPS, VPN y comunicaciones unificadas, la formación de clústeres, identificación del contexto con etiquetas de grupos de seguridad (detección de identidad) o facilitar el enrutamiento dinámico y VPN entre sitios en función del contexto.

Los dispositivos Cisco ASA pueden implementar las siguientes funcionalidades de filtrado[21]: filtrado de paquetes con estado, control e inspección de contenido, control de acceso basado en usuario, auditoria de sesión, módulos hardware específicos de seguridad, filtrado por reputación y categoría, comunicaciones unificadas criptográficas, prevención de denegación de servicio, correlación de tráfico y VPN, entre otras.

Las características técnicas de este firewall son:

- Rendimiento del firewall hasta 1 Gbps.
- Capacidad multiservicio.
- 8 x 1 Gigabyte Ethernet.
- 1 RU.

Una de las vulnerabilidades que sufre este equipo es el enfrentarse a nuevo malware. Son necesarias nuevas licencias, las cuales tienen un coste económico elevado, para actualizar los equipos, y esto debe hacerse conectándolos a internet. Además, en el año 2018 se darán de baja estos equipos en el ET puesto que desde CISCO se va a dejar de ofrecer soporte a los equipos, por lo que es necesario buscar otro equipo que lo sustituya.

[20] Por ejemplo, aplicaciones como YouSendIt, SalesForce, Messenger o Skype, entre otros, en las que el usuario puede utilizar diferentes funcionalidades y hacer uso de diferentes recursos.

[21] Las distintas funcionalidades vienen explicadas en el Anexo 1.

5.2. Estudio de los routers

Cuando hablamos de routers, podemos estar hablando de dos tipos de routers: negros o rojos, dependiendo de su posición en la red, antes o después del cifrador. En el plan MC3 vienen definidas las características que deben poseer los routers que componen la red desplegable del ET:

- Soporte de Multicast en modo *Sparse*.
- Soporte de BGP.
- Capacidad de montar tarjetas de red de fibra monomodo LC a 1GB.
- Capacidad de disponer de al menos dos conexiones directas con otros dos MNE, s.

Actualmente se encuentran en dotación diferentes modelos de routers, ya que según se han ido necesitando se han ido comprando atendiendo a las necesidades, tanto técnicas como económicas, del momento. Los dos modelos más comunes son el CISCO 2911 y el CISCO 3945.

Figura 13. Router CISCO 2911 [11]

Como se puede ver en la Figura 13, el router CISCO 2911 dispone de 4 interfaces de red Giga Ethernet, así como de 2 puertos RJ-45 y 2 de FO a 1 Gb.

Con motivo de disponer de mayor flexibilidad de configuraciones, se requiere que disponga de un número elevado de bahías, por lo tanto, se han ido adquiriendo versiones más modernas como el CISCO 3945. La mejora se ha producido con el aumento de los puertos RJ-45 incluyendo 2 capaces de utilizar conectividad SFP.

Aunque actualmente las capacidades de procesamiento y distribución de los routers no han sido sobrepasadas, con la solución que se va a plantear a los fallos encontrados en el apartado 3.2 puede ser necesario considerar la adquisición de un router más potente. Esta opción se valorará en el apartado 6.8.

6. Soluciones propuestas

En el siguiente apartado se van a exponer y valorar las posibles soluciones que propuse, junto con los oficiales correspondientes, para afrontar los problemas que han ido apareciendo al realizar el estudio de los diferentes equipos en los apartados 3, 4 y 5.

6.1. Solución a los problemas encontrados en los servidores HP PROLIANT DL380P GEN8

En el estudio de los servidores HP PROLIANT DL380P GEN8 se han encontrado dos problemas: sobrecalentamiento de los servidores y rotura del cable de la fuente de alimentación. Aunque los problemas de refrigeración afectan a todo el nodo, es en los servidores donde se muestra como un aspecto crítico que se debe tomar en consideración.

Ante el primer problema encontrado, el sobrecalentamiento de los servidores, se pueden plantear dos soluciones: aumentar el espacio físico entre los servidores y mantener la refrigeración como hasta ahora en tiendas con aire acondicionado o cambiar el tipo de refrigeración a una de refrigeración líquida. Al aumentar el espacio físico, la disipación del calor se haría de manera más sencilla y solo supondría aumentar el tamaño del *rack* o dividir el equipo en más *racks*, aunque la mejoría solo se notaría en ambientes con una temperatura no demasiado alta pues a los 95ºC el equipo se apaga. La solución de la refrigeración líquida supondría también aumentar el tamaño del *rack* y además incrementaría el coste de los nodos, pues sería necesario adquirir este tipo de refrigeración. La refrigeración líquida es un método más eficiente para la disipación de calor[22].

Como se ha visto, ambas soluciones suponen aumentar el tamaño del *rack*, lo que en la práctica equivaldría a separar el equipo en dos *racks* para que sea factible su traslado. Este aumento supone incrementos de coste, que se detallan en el Apartado 7 de esta memoria. Por tanto, se recomienda la refrigeración líquida para solucionar el problema de sobrecalentamiento de los servidores HP PROLIANT DL380P GEN 8. El estudio de la incorporación de la refrigeración líquida en los Nodos de SIMACET de BRI puede ser objeto de un TFG.

Respecto a los problemas por la rotura del cable de la fuente de alimentación la solución planteada es la de utilizar cables con fijación por tornillos para asegurarlos. Para ello los equipos deben ir al 2º Escalón[23] para incorporar este tipo de fijación. Además, también se incluye la recomendación de utilizar canalizaciones

[22] Empresas como Google, Facebook o eBay y administraciones como la NSA utilizan este tipo de refrigeración.

[23] Unidad encargada de realizar modificaciones básicas en lo relativo al hardware de los equipos.

de cables. El coste de estas modificaciones es despreciable, por lo que no se van a incluir en el Apartado 7.

También se ha valorado la sustitución de los servidores por otro modelo equivalente de otra empresa, pero se ha descartado porque se enfrenta a los mismos problemas y no se observaría una mejora o solución a los problemas aparecidos.

6.2. Solución a los problemas encontrados en el array de discos HP STORAGEWORKS P2000 G3

Como se ha descrito a lo largo del trabajo, los equipos del Nodo SIMACET V.5 BRI se encuentran duplicados para conseguir la alta disponibilidad del sistema que se busca, pero en el array de discos esto no es así, ya que la información se guarda en un solo equipo. En este apartado se van a valorar diferentes opciones basadas en la idea de utilizar un segundo array de discos.

La primera opción planteada es la de utilizar un segundo array de discos en el mismo *rack* en el que se encuentra el resto de los equipos del nodo. La ventaja que presenta es que se consigue la redundancia en el servicio deseada, así como mayor espacio de almacenaje por si pudiera ser necesario. Esta solución sería la de más fácil aplicación, puesto que solo consistiría en la compra de un segundo array de discos y en la implementación del protocolo de alta disponibilidad para que los dos array de discos trabajen de manera conjunta. Por el contrario, la desventaja que supone almacenar físicamente toda la información en el mismo lugar físico es evidente, ya que ante un desastre natural o un ataque se podría perder toda la información.

Una segunda opción, sería una corrección de la primera. Esta consistiría en sacar el segundo array de discos del mismo entorno en el que se encuentra el nodo (y el primer array de discos). Con ello lo que se conseguiría es solucionar los problemas que presenta la primera opción, pero surgiría el problema del volcado de datos. Todos los servidores virtuales almacenados en el array de discos del nodo y toda la información de usuario almacenada en la red se clonaría en el array de discos 2 (separado físicamente del nodo). Esta información contiene a todos los servidores virtuales funcionando en ese momento, lo que supone un elevado volumen de datos a transmitir y la red no dispone de capacidad suficiente para una transmisión en tiempo real (los datos “pesan” demasiado como para poder llevar a cabo un clonado diario). Por lo tanto, conviene arbitrar un procedimiento cada 2 o 3 días y fuera del horario de trabajo de los usuarios. El problema surgido de realizar un clonado cada varios días es que, si se pierde la información el tercer día antes de realizar el clonado, se perderían los datos de 3 días y eso no es asumible en combate.

Existen diferentes formas de conseguir reducir el volumen de datos que se necesita transmitir. Por ejemplo, un *Snapshot* permite guardar el estado actual de una máquina virtual y permite retornar a él en cualquier momento (es el equivalente a los puntos de restauración de Windows). Incluye: el contenido de la memoria de la máquina virtual, las propiedades de la máquina y el estado del disco duro. Para las

máquinas clonadas se consigue una reducción importante de la memoria utilizada para guardar los datos de una segunda, tercera o más máquinas. Otra manera sería priorizar los datos tratando de minimizar el impacto sobre el usuario y su trabajo.

También estaría el problema de que, aunque se conservaran los datos si el nodo hubiera sido destruido, no habría forma de utilizarlos al no disponer de los equipos necesarios. Por ello, una tercera solución sería la utilización de un nodo de reserva, conectado y funcionando a la par que el principal, como nodo de respaldo. Este nodo de reserva no debería ser necesariamente un nodo de la misma entidad que el empleado, sino que bastaría con uno de menor entidad. Por ejemplo, un Nodo de División necesitaría un Nodo de Brigada o un Nodo de Brigada un PUT (aún no se encuentra virtualizado).

6.3. Solución a los problemas encontrados en el servidor de backup

El único problema observado es la caducidad de las licencias y el alto coste[24] de su renovación. No hay más solución que comprar las licencias cuando estas caduquen, ya que debido a que el software libre no es acreditable hay que adquirirlas para conseguir que los equipos funcionen y sean acreditables.

6.4. Solución a los problemas encontrados en el switch

No se ha encontrado ningún problema.

6.5. Solución a los problemas encontrados en el sistema de alimentación

Ante el problema surgido en el apartado 3.5 Estudio del Sistema de alimentación como solución se propone la adquisición de un segundo SAI. Esto es debido a que, puesto que en el diseño de los equipos el SAI no está contemplado como un elemento alternativo para proporcionar energía al nodo, sino que lo hace como fuente de energía temporal para dar al administrador tiempo para conseguir suministro de corriente eléctrica, es necesario aumentar el tiempo que se proporciona energía a estos. También se debe tener en cuenta que al añadir un segundo SAI y no adquirir uno de mayor potencia, lo que se consigue es redundar este servicio, como se ha hecho con el resto de equipos del nodo.

En lo que respecta a los sistemas de alerta, se propone lo siguiente:

1º La sustitución del led de aviso por una luz rotativa de señalización. La utilización de este objeto proporcionaría un aviso claro e inmediato a los administradores de que ha habido un corte del suministro eléctrico en el equipo.

[24] El coste de la licencia de Backupexec es de 1673,19€.

2º La incorporación de un sistema de altavoces que amplifique el sonido de la alarma. Aunque con la luz pudiera parecer suficiente, se recomienda duplicar los sistemas de alarma. Este tipo de alarma serviría para que en caso de que no se encontrara ningún administrador junto al equipo estos pudieran ser alertados del fallo del suministro eléctrico.

3º La adquisición de otro modelo de SAI diferente. El problema que plantea el cambio de modelo es que sería necesario un concurso público de adquisición de material por parte del MALE. Esta solución, aunque válida, es la menos deseable ya que dilata en el tiempo su aplicación y tiene mayores costes en comparación con los beneficios que podría reportar.

6.6. Solución a los problemas encontrados en el software

En el apartado 4, tras el estudio realizado, han aparecido varios problemas. El primero de ellos era que las tarjetas de red del controlador de dominio se deshabilitaban cuando estos se reiniciaban. La solución que se viene aplicando hasta ahora ha sido la de volver a habilitar manualmente la tarjeta de red. Este es un paso sencillo por lo que en este apartado no se va a plantear ninguna solución alternativa al tratarse de una solución rápida y sencilla, al contrario de lo que supondría realizar un estudio del código de programación de los controladores de dominio y solucionar el problema. Esta solución se escapa de los objetivos del presente trabajo puesto que se requieren unos conocimientos muy técnicos en otras materias, como informática y programación, no incluidas en esta titulación y podrían proponerse o plantearse como un TFG de las mismas.

La falta de conocimiento de los usuarios sobre el sistema se soluciona con cursos de formación en nuevas tecnologías. Estos cursos pueden ser impartidos por los administradores de los nodos, consiguiendo solucionar este problema sin incurrir en ningún coste. Ante el problema expuesto de EXCHANGE, que también podría ser el de otra aplicación, la mejor solución, y reforzando las ideas recogidas en los apartados 6.2 y 6.3, es disponer de copias de seguridad de los archivos realizados y modificados. Puesto que las máquinas virtuales se corrompen con mayor facilidad, esto puede resolverlo.

Por último, respecto al problema de las licencias, es un problema que, aunque la solución es clara, no es sencilla de aplicar puesto que requiere un desembolso importante de dinero en el mantenimiento de las licencias. Como se mostraba en el estudio realizado en el apartado 4, el software libre queda descartado como posible solución puesto que no cumple los requisitos OTAN. Estos requisitos son imprescindibles si se quiere contar con la certificación necesaria para poder integrarse en su red y manejar su información clasificada. Por tanto, aunque se pudiera utilizar software libre para los equipos nacionales que no tengan pensada una posible interacción con la red OTAN, se desaconseja porque provocaría problemas de interacción entre los equipos a nivel nacional.

6.7. Solución a los problemas encontrados en el firewall

Ante el problema encontrado en el apartado 5.1, existen dos posibles soluciones: comprar la siguiente versión de firewall y las licencias de CISCO o comprar un firewall de otra empresa del sector (Palo Alto). Para ello a continuación se va a analizar cuáles son las características de la versión de Palo Alto.

El firewall PA-3020[25] [12] se diferencia del resto de firewalls en el software utilizado para funcionar, utilizando uno completamente diferente al del resto de la industria, como se va a explicar a continuación. Este firewall no se encuentra actualmente en servicio en el ET, pero se está estudiando su incorporación.

Como se mencionaba en el apartado 5.1, el firewall PA-3020 utiliza la nueva tecnología NGFW (*Next Generation FireWall*) disponible para firewalls. La tecnología App-ID permite ver las aplicaciones en la red y aprender cómo funcionan, sus características de comportamiento y su riesgo relativo. Las aplicaciones y las funciones de aplicación se identifican mediante múltiples técnicas, como firmas de aplicación, descifrado (si es necesario), decodificación de protocolo y heurística. Esto permite un control granular, por ejemplo, permitiendo solo cuentas sancionadas de una determinada aplicación, o permitiendo la mensajería instantánea, pero bloqueando la transferencia de archivos.

La arquitectura que usa PA-3020 es la arquitectura Single-Pass, que permite la clasificación completa y contextual del tráfico, seguida de un conjunto de opciones de prevención de amenazas y asegurando su cumplimiento. La arquitectura debe su nombre a que clasifica y controla el tráfico en un "paso único" a través del firewall.

El firewall PA-3020 realiza un análisis en *streaming* de los datos que pasan a través de él. Para conseguir detectar el malware se hace lo siguiente tras analizar los datos: en el caso de que se detecte malware conocido por el firewall este es bloqueado, en el caso de que no sea así se envía a lo que se denomina *Sandbox* (en la que se ejecuta en una máquina virtual) y en caso de que sea bueno se deja pasar, y en caso contrario se bloquea y se actualizan las firmas en el resto de firewalls conectados a la misma red.

La ventaja de este firewall es su principal inconveniente para su aplicación en las redes desplegables. Al llegar hasta la Capa 7[26], proporciona una gran versatilidad para la configuración de seguridad para cada usuario, pero, al ser variables los requisitos de los usuarios, hace que la complejidad a la hora de configurar los usuarios requiera de un mayor número de administradores o de más tiempo en la preparación de una maniobra. Estos firewalls son utilizados por diversos organismos estatales como la Guardia Civil o la Armada, pero se utilizan en lugares con una

[25] Ver Anexo 5 Características PA-3200.
[26] En el modelo de capas OSI la Capa 7 es la Capa Aplicación.

configuración permanente y serían de gran utilidad en los nodos permanentes o en los CECOM.

Como conclusión, ante las dos opciones que se planteaban al principio de este apartado, y a pesar de los inconvenientes referidos anteriormente, se recomienda su adquisición por parte del ET para su incorporación a las redes militares. Ante la necesidad de adquirir nuevos terminales por la caducidad de los actuales equipos, este es el equipo más económico y con mejores prestaciones. Además permitiría aprovechar la integración con otras redes como la de la Guardia Civil y así proporcionar actualizaciones contra las amenazas de malware más recientes.

6.8. Solución a los problemas encontrados en los routers

Atendiendo a lo expuesto en el Apartado 6.2, puesto que sería necesario aumentar demasiado el tamaño de la red para poder soportar el elevado tráfico de datos que se propone en la segunda opción de este apartado, solo cabe descartar la idea de adquirir routers más potentes para dotar de mayor capacidad a la red. El aumento en conexiones de cables no es interesante para un puesto de mando de Brigada, ya que demoraría su despliegue y aumentaría sus necesidades logísticas.

7. Costes

Tras las soluciones que se han ido planteando en el Apartado 6, han surgido nuevos posibles costes que sería necesario asumir para poder completar los equipos. El ET se beneficia de realizar compras en lote de los diferentes equipos, además también sería necesario tener en cuenta las licencias[27] de estos, por tanto, los costes que se reflejan a continuación son solo una posible aproximación. También se debe tener en cuenta que el único equipo propuesto diferente de los que se encuentran en uso actualmente es el firewall PA-3200, en el que se conseguiría un ahorro del 25% con respecto al firewall CISCO ASA 5525X.

Equipo		Precio
Servidor HP PROLIANT DL380P GEN8		1500 €
Array de discos HP STORAGEWORKS P2000 G3	Equipo completo	9900 €
	Discos por separado	730 €
Servidor de backup HP STOREONCE 2700		14500 €
SAI R/T 3000VA		1090 €
Firewall PA-3200		6000 €
Rack		3000 €
Router 3945		4350 €
Router 2911		950 €

Tabla 1. Desglose de costes de los equipos. Fuente: elaboración propia.

Por tanto el coste de las modificaciones propuestas sería de aproximadamente 41.790[28] € atendiendo a los precios de la Tabla 1.

Al analizar los costes se debe tener en cuenta que, las mejoras propuestas no buscan obtener beneficios económicos para el ET, sino que buscan aumentar sus capacidades y que esto se haga con un coste asumible. El único beneficio económico obtenido con los Nodos de SIMACET V.5 se consiguió con la virtualización, y no durante el trabajo. Aunque desde un punto de vista inicial del proyecto se buscaba también reducir el coste de los nodos, se descartó pronto esta línea de trabajo ya que no era compatible con mejorar los defectos de los nodos.

[27] Los precios de las licencias que paga el ET no son públicos ni se pueden incluir en este documento. Además estos son material clasificado.

[28] Precio para 1 Array de discos HP STORAGEWORKS P2000 G3, 10 discos para HP STORAGEWORKS P2000 G3, 1 Servidor de backup HP STOREONCE 2700, 1 SAI R/T 3000VA, 1 Firewall PA-3200 y 1 *Rack*.

8. Conclusiones

Como consecuencia de haber realizado este TFG se han llegado a varias conclusiones. Aprovechando que SIMACET V.5 aún no ha sido introducido en las unidades del ET se propone que estas conclusiones se apliquen antes de su implementación, para así conseguir un ahorro en costes futuros y disponer de nodos con las mejores prestaciones.

La primera conclusión obtenida es la necesidad de incorporar una segunda SAI en el Nodo de SIMACET V.5 para así tratar de resolver la mayoría de los problemas aparecidos en los equipos debido a los cortes de corriente. Esta es una solución de poco coste y fácil implementación, que presentaría grandes ventajas a los nodos. No se debe olvidar, la implementación de las medidas referidas en el apartado 6.5 sobre los sistemas de alerta.

La segunda conclusión a la que se ha llegado es la necesidad de mejorar la refrigeración de los nodos, dejando más espacio físico entre los servidores (separándolos en 2 *racks* para que no sean demasiado pesados) e introduciendo un sistema de refrigeración líquida.

Por último, pero no menos importante, otra de las conclusiones obtenidas es la de conseguir redundancia en el almacenamiento de los datos. Para ello, se propone, o bien incorporar un nodo de reserva en la Red desplegable o incorporando físicamente un segundo array de discos (externo al nodo), teniendo en cuenta que la solución idónea sería la de utilizar un nodo de reserva. Estos últimos aún no se han virtualizado, lo que podría estudiarse en futuro TFG.

8.1. Propuestas de futuros trabajos

Durante la elaboración del TFG han surgido problemas, en los que la búsqueda de una posible solución podría ser objeto de un futuro TFG. Este es el caso de los PUT, que se plantean como una solución a uno de los problemas tratados en el presente trabajo, pero que aún no cumplen con la característica de estar virtualizados.

También, como se ha indicado anteriormente en el trabajo, la implantación de refrigeración líquida en los Nodos de SIMACET V.5 puede ser una futura línea de trabajo para la realización de un TFG.

Bibliografía

1. Doctrina, Mando de Adiestramiento y. *Empleo de la Unidad de Transmisiones de la Brigada.* 2004.

2. JCISAT. *ARET-MC3-CIS-GU.* Octubre 2013.

3. Ingenieros, Academia de. *SIMACET.* 2017.

4. CAPACITY Information Technology Academy. [En línea] 2016. [Citado el: 16 de 09 de 2017.] http://blog.capacityacademy.com/2012/08/07/que-es-la-virtualizacion-y-cuales-son-sus-beneficios/.

5. Márquez, Comandante Jose Manuel Gallego. *PROCEDIMIENTO BACK UP.* Mahón (Menorca) : REGIMIENTO DE TRANSMISIONES 21, 2017.

6. [Online] [Cited: 2 10 2017.] **https://www.pcmag.com/article2/0,2817,2421554,00.asp .**

7. CNET. [Online] [Cited: 21 09 2017.] **https://www.cnet.com/products/hp-storeonce-2700-backup-nas-server-8-tb-bb877a/specs/.**

8. Telesis, Allaied. Switch AT-X610-24TS. [Online] [Cited: 03 10 2017.] **https://www.alliedtelesis.com/products/switches/x610-24tsx-poe#**.

9. *Virtualización.* LAPEÑA, TTE SERGI HERAS. Hoyo de Manzanares : s.n., 2018**.**

10. Explotación, Sgto 1º Administrador Sección de. *Firewall CISCO ASA 5525X.* 27 de 09 de 2017.

11. CISCO Packet Tracer. *Router CISCO 2911.*

12. Garijo, Juan Luis. *Firewall PA-3200.* 29 de 09 de 2017.

13. Palo Alto Networks. www.paloaltonetworks.com. [Online] [Cited: 27 09 2017]. **https://www.paloaltonetworks.com/.**

14. Centro Criptográfico Nacional. *Seguridad en Cortafuegos CISCO ASA (CCN-STIC-651).* 2015.

15. FNAC. [Online] 2017. [Cited: 09 10 2017.] **https://www.fnac.es/mp3321921/Allied-Telesis-AT-X610-24TS-X-60-switch/w-4.**

16. ServerSupply.com Inc. Server Supply. [Online] 2004. [Cited: 10 09 2017.] **https://www.serversupply.com/MEMORY/PC3-10600/16GB/HP/647901-B21.htm.**

Anexos

Anexo 1. Tipos de Filtrado

Las tecnologías o métodos [14] que se utilizan para implementar los cortafuegos que existen en la actualidad son básicamente:

- Filtrado de paquetes sin estado: el cortafuegos comprueba únicamente las cabeceras de las paquetes y segmentos de nivel de red y transporte (nivel 3 y 4 de OSI) sin tener ninguna consideración en cuanto al estado de la conexión, negociaciones dinámicas de sesiones y puertos.
- Filtrado de paquetes con estado: en este caso el cortafuegos almacena el estado de las conexiones individuales para comprobar que siguen un comportamiento establecido.
- Filtrado de paquetes con estado y control e inspección de contenido: el cortafuegos, reensamblando las sesiones UDP y TCP, inspecciona el contenido a nivel de aplicación (nivel 7 de OSI).
- Sistema de prevención de intrusiones de red: se analiza el tráfico y se compara con una base de datos de actividad de código dañina conocida. Estas anomalías se pueden detectar por paquetes únicos o por un patrón de tráfico constituido por varios paquetes.
- Análisis de comportamiento de red: el cortafuegos analiza el tráfico de red durante un tiempo para establecer un patrón de comportamiento normal. Este análisis tiene en cuenta el ancho de banda utilizado, tipos de aplicaciones y protocolos. El patrón definido como normal debe redefinirse continuamente.
- Pasarela a nivel de aplicación (proxy): el cortafuegos actúa como intermediario entre el cliente y el servidor. El proxy, haciéndose pasar por al usuario, reenvía el tráfico hacia el servidor y las respuestas de este, una vez evaluadas, decide qué hacer con ellas.

Anexo 2. Características AT-X610-24TS

Allied Telesis AT-X610-24TS/X-60 [15]. Capa del interruptor: L3. Puertos tipo básico de conmutación RJ-45 Ethernet: Gigabit Ethernet (10/100/1000). Estándares de red: IEEE 802.3, IEEE 802.3at. Tabla de direcciones MAC: 32000 entradas. Algoritmos de seguridad soportados: SSH, SSL/TLS

Características:

Capa del interruptor: L3

MIB, soporte: Sí

Calidad de servicio (QoS): Sí

Multidifusión: Sí

Administración basada en web: Sí

Cantidad de puertos básicos de conmutación RJ-45 Ethernet: 24

Puertos tipo básico de conmutación RJ-45 Ethernet: Gigabit Ethernet (10/100/1000)

Cantidad de puertos SFP: 4

SFP + Cantidad de puertos: 2

Jack de entrada CD: Sí

Estándares de red: IEEE 802.3, IEEE 802.3at

Bidireccional completo (Full dúplex): Sí

Soporte de control de flujo: Sí

Espejeo de puertos: Sí

Adición de vínculos: Sí

DHCP, cliente: Sí

DHCP, servidor: Sí

IGMP: Sí

Protocolo de árbol de expansión: Sí

Soporte VLAN: Sí

Tabla de direcciones MAC: 32000 entradas

Número de colas: 8

Jumbo Frames: Sí

Algoritmos de seguridad soportados: SSH, SSL/TLS

Lista de Control de Acceso (ACL): Sí

Soporte SSH/SSL: Sí

Protocolos de gestión: SNMPv1, v2c, v3

Protocolo de conmutación: IGMPv3, IPv6, MLDv2

Montaje en *rack*: Sí

Indicadores LED: Sí

Certificación: UL60950-1, CAN/CSA-C22.2, No. 60950-1-03, EN60950-1, EN60825-1, AS/NZS, 60950.1

Apilable: Sí

Consumo energético: 92W

Energía sobre Ethernet (PoE): No

Medidas: Ancho: 44 cm (ancho) x 42 cm (profundidad) x 4,4 cm (altura)

Anexo 3. Características tarjetas RAM 647901-B21 - HP 16GB

Nombre del producto: 16GB DDR3 SDRAM MEMORY MODULE

Información técnica [16]**:**

STORAGE CAPACITY: 16GB

MEMORY TECHNOLOGY: DDR3 SDRAM

CHIPS ORGANIZATION: X4

NUMBER OF MODULES: 1 X 16GB

BUS SPEED: 1333MHZ DDR3-1333/PC3-10600

DATA INTEGRITY CHECK: ECC

SIGNAL PROCESSING: REGISTERED

RAM FEATURES: DUAL RANK, LOW VOLTAGE

CAS LATENCY TIMINGS: CL9

TYPE: DRAM

UPGRADE TYPE: SYSTEM SPECIFIC

PLATFORM SUPPORT: HP PROLIANT SERVER

Anexo 4. Características SAI R/T300VA G2

Referencia	Sistema de alimentación ininterrumpida HP R/T3000 G2 2U L620, alta tensión, NA/JP
Detalles técnicos	
Segmentos de carga	2
Conexión eléctrica de entrada	NEMA L6-20P
Conectividad	
Puerto serial	Puertos estándar DB-9 y USB. Módulo de red SAI HP
Conexiones eléctricas de salida	(6) IEC 60320 C13; (2) IEC 60320 C19; (1) NEMA L6-20R
Peso y dimensiones	
Peso	37000 g
Condiciones ambientales	
Alcance de temperatura operativa	10 - 40 °C
Temperatura	0 - 25 °C
Humedad relativa	20 - 80 %
Humedad (en almacenaje)	5 - 95 %
Altitud operacional	Hasta 2.000 sobre el nivel del mar
Altitud no operativa	15.000 sobre el nivel del mar
Aprobaciones reguladoras	
Seguridad	FCS, UL, CSA, VDE, NEMKO, FIMKO, DEMKO, SEMKO, NOM (*Safety Markings*); UL1778; CSA22.2 No.107.1, No.107.2, No.950; CB Bulletin No.86AI; EN50091-1; EN60950; EMKO-TSE207/95; NOM-019-SCFI-1993 (*Safety Certifications*)
Sistema operativo/software	
Software para comunicación	*HP Power Protector*
Batería	
Tipo de batería	Maintenance-free, sealed, valve-regulated lead acid (VRLA)
Batería *hot-swappable*	Sí
Otras características	
Dimensiones (Ancho x Profundidad x Altura)	445 x 635 x 89 mm
Voltaje nominal de salida	200-208 V

Anexo 5. Características PA-3200

Las características técnicas del producto son las siguientes:

- Rendimiento de firewall de 2 Gbps (con App-ID habilitado).
- Rendimiento de prevención de amenazas de 1 Gbps.
- Velocidad de transferencia IPSec VPN de 500 Mbps.
- 250.000 sesiones máximas.
- 50.000 nuevas sesiones por segundo.
- 1.000 túneles VPN IPSec / interfaces de túnel.
- 1.000 usuarios de SSL VPN.
- 10 routers virtuales.
- 1/6 sistemas virtuales (base / max2).
- 40 zonas de seguridad.
- 2.500 número máximo de pólizas.

Anexo 6. Entrevistas

Como política interna de protección de datos del RT-21, este no quiere que aparezcan los nombres completos de los subordinados entrevistados, por tanto, no aparecerá más que su empleo y primer apellido.

Anexo 6.1. Entrevista Sargento 1º Zuluaga administrador HP PROLIANT DL380P GEN8

Como administrador del equipo durante los últimos 5 años y experto en el equipo HP PROLIANT DL380P GEN8, ¿podría hacer un resumen de las características del equipo?

Dispone de una memoria RAM de 192 GB.

Tipo de procesador Intel Xeon CPU E5-2650 0 @ 2 GHz

Número de procesadores: 16

¿A cuántos usuarios puede dar servicio? ¿Diría que tiene suficiente capacidad?

Lo normal es que por su entidad dé servicio a entre 70 y 80 usuarios, pudiendo llegar en algún ejercicio específico a un número mayor de usuarios. Por norma general se reservan 50 direcciones para los diferentes dispositivos de la red, como pueden ser las impresoras, etc. Eso hace que se utilicen unas 130 direcciones IP de las 256 del *pull* de direcciones que tiene asignado el nodo. Por tanto, el equipo nunca llega a utilizar todos las direcciones, siempre sobran.

Entonces ¿Cree que está desaprovechado el servidor dentro del nodo en la versión v.5? Porque tiene capacidad para dar servicio a más usuarios y además no se utilizan todos los recursos de los que dispone el servidor.

No, está bien aprovechado. Uno más grande no es necesario, ya que la entidad de la unidad no necesita un servidor con mayor capacidad, pero es necesario tener un servidor con suficiente capacidad para poder trabajar. Por otro lado, sí que es verdad que la memoria interna de los servidores no se usa, pero esto se debe a que representa poco espacio de almacenamiento en comparación con lo proporcionado por el array de discos.

¿Cuáles son las piezas más vulnerables?

El equipo funciona bien y tiene la capacidad adecuada, el único problema son los conectores. La clavija de entrada de la fuente de alimentación es la que mayores problemas presenta. En general son los conectores externos los más vulnerables.

Entonces, ¿cuáles diría que son los fallos más comunes?

Como he dicho, solo suelen fallar los conectores externos. Tal vez otro de los problemas es el sobrecalentamiento. En verano cuando hace más calor y es más difícil refrigerar el equipo este puede apagarse debido a un exceso de temperatura.

¿Cuál cree que es la solución a los fallos más comunes?

El principal problema es que las pestañas de la entrada de la fuente de alimentación acaban pasadas de rosca, debido a que no está diseñada para montarse y desmontarse. Además el problema se agrava cuando el nodo está sobre plataforma vehicular, ya que el equipo se encuentra mal distribuido y está demasiado pegado a la pared, con lo que el administrador no tiene visibilidad cuando accede a la parte trasera de los equipos para conectar los diferentes conectores.

Además también sería necesario buscar una forma mejor de refrigerar los equipos, tal vez con refrigeración líquida o con equipos de aire acondicionado más potentes.

¿Aumentar la capacidad de algún componente puede ser la solución o es necesario otro nuevo?

No es necesario. Las capacidades que posee son suficientes.

El nodo posee dos servidores iguales. ¿Es capaz de funcionar un servidor con todos los servicios si el otro cae? ¿Cómo lo hace para compartir los servicios?

Si, el nodo busca tener redundancia en los servicios que ofrece. Para ello debe estar el habilitado el protocolo *High Availability*.

¿Cuál es su opinión sobre el equipo? ¿Está satisfecho?

Es buena, mis compañeros y yo estamos satisfechos con el equipo y no cambiaríamos ningún componente, aparte de los conectores y el sistema de refrigeración como ya he dicho antes.

Anexo 6.2. Entrevista Sargento 1º Zuluaga administrador HP STORAGEWORKS P200 G3

¿Qué capacidades tiene este equipo?

El array de discos está formado por 24 discos de 900 GB, esto le da 21,6 TB de almacenamiento.

¿Cuáles son las piezas más vulnerables?

Al salir al campo, los discos se llenan de polvo y no funcionan. Los golpes también son un problema. Pero es básicamente lo que le pasa a cualquier disco duro de los que podemos encontrar en la calle.

¿Cuáles son los fallos más comunes?

El fallo más común es que el disco se quede inoperativo por la suciedad del ambiente en el que se utilizan estos equipos.

¿Cuál cree que es la solución a los fallos más comunes?

Si no se trabajara en la misma habitación no entraría polvo, al menos no tanto. No hay problema en trabajar desde otra habitación, es igual de cómodo trabajar sin estar en la misma habitación.

¿A qué se refiere con trabajar desde otra habitación?

Me refiero a que si los administradores trabajaran en una modular diferente a la que se encuentran los equipos entraría menos polvo.

¿Es suficiente tener solo un servidor de este tipo o sería conveniente tener dos aunque fueran de menor capacidad?

Para una brigada es suficiente espacio de almacenamiento.

Y si pensáramos en redundar los servicios, como se hace normalmente con la mayoría de los equipos en el ET, ¿no cree que sería necesario tener un segundo array para guardar una copia de seguridad de los archivos separada físicamente del resto de los equipos?

Sí, viéndolo desde ese punto de vista sí.

¿Cuál es su opinión sobre el equipo? ¿Está satisfecho?

Buena, porque no suele presentar problemas, y en el caso de que aparezcan son de fácil solución. Solo con cambiar el disco que ha fallado se soluciona.

Anexo 6.3. Entrevista Sargento 1º Cebolla administrador Servidor HP STOREONCE 2700

¿Por qué el nodo tiene este tipo de servidor, si ya posee almacenamiento suficiente en el array de discos? ¿Cuál es su función?

Es la cabina de discos de *backup*, se utiliza para realizar copias de seguridad de los archivos. Su funcionamiento sería como si fuera un simulador de librería de brazo robótico. El solo se va organizando para guardar la información en las diferentes carpetas.

¿Qué capacidad tiene este servidor de backup?

Tiene un espacio de almacenamiento de 8 TB, ya que tiene 4 discos de 2 TB.

¿Tiene suficiente capacidad? ¿Se están aprovechando los recursos del equipo?

Sí.

¿Cuáles son las piezas más vulnerables?

Hasta el momento no hemos encontrado ningún componente que funcione mal, no suele fallar.

¿Cuáles son los fallos más comunes?

El problema es que funciona con el programa Backupexec que necesita licencias para funcionar y no siempre tiene la licencia actualizada.

¿En qué consiste Backupexec?

Es el software propio del equipo encargado de gestionar las copias de seguridad del servidor de backup.

¿Qué pasa si el equipo no tiene licencia de Backupexec? ¿Puede seguir funcionando?

Si no tiene licencia hay un tiempo de licencia de prueba. Durante este tiempo puede seguir funcionando porque tiene una licencia temporal, pero es necesario renovarla para que acrediten los equipos.

¿Cómo se renueva?

Es necesario solicitarlo al Parque Central de Transmisiones, estos conceden la licencia temporalmente, normalmente para un año. El problema es que es una cosa cara.

¿Es suficiente tener solo un servidor de este tipo o sería conveniente tener dos aunque fueran de menor capacidad?

Mejor uno porque va bien y como he dicho anteriormente no suele fallar. No es necesario gastar el dinero en otro.

¿Cuál es su opinión sobre el equipo? ¿Está satisfecho?

Buena, va bien. Lo único las licencias, porque al final son necesarias para tener el servidor operativo.

Anexo 6.4. Entrevista Sargento 1º Cebolla administrador Switch AT-X610-24TS

¿Qué capacidad tiene este modelo de switch?

Es un switch de 24 puertos Ethernet y un puerto de fibra óptica.

¿Son suficientes puertos?

Si tenemos en cuenta que el nodo tiene dos switches hablamos de 48 puertos Ethernet. Estas son suficientes conexiones, ya que normalmente creamos switches virtuales para conseguir capacidad para todos los usuarios del nodo.

¿Cuáles son las piezas más vulnerables?

Los conectores, pero no es común que se rompan. Ha pasado alguna vez, pero hay puertos Ethernet de sobra para poder utilizar otro.

¿Cuál es su opinión sobre el equipo? ¿Está satisfecho?

Si fuera Cisco sería más homogéneo respecto al resto de los equipos, ya que la forma de programar sería igual para todos los equipos. Los cursos se dan con equipos Cisco, y después en la unidad nos encontramos con que los equipos son AT-X610 con lo que, aunque la teoría sea igual, después el manejo varía.

Anexo 6.5. Entrevista Capitán D. José Miguel Domínguez Rodríguez administrador SAI

¿Qué capacidad tiene el SAI?

3000VA.

¿Cuál diría que es el principal problema del SAI?

Son equipos delicados, necesitan mucho mantenimiento. Si este no se hace, la carga cada vez es más corta. Supuestamente el modelo actual debe mantener alimentado al nodo durante 30 minutos, pero al final la duración real que tienen son de 10 minutos.

¿Cómo cree que se podría solucionar esto?

Realizando un mantenimiento adecuado. Las baterías son el elemento más delicado. Para que el mantenimiento sea adecuado deben cargarse y descargarse completamente al menos una vez al mes.

¿Cree que hay algún otro aspecto que sería mejorable en el equipo a parte de las baterías?

Suena poco si se quedan sin batería. Más de una vez se nos han apagado porque se ha ido la luz y no nos hemos enterado a tiempo. Hay que tener en cuenta que dentro de una modular o en un *shelter* el ruido de los administradores o el de los equipos por estar funcionando hace que no se escuche casi.

¿Cuál cree que es la solución a los fallos más comunes?

Cambiar la señalización cuando se están quedando sin batería. Imprescindible.

¿Cuál es su opinión sobre el equipo? ¿Está satisfecho?

No mucho. Es un aspecto que necesita ser revisado.